

POLITIQUE GNERIQUE DE GESTION DES COMPTES ET DES MOTS DE PASSE

Ce document a pour objectif de décrire la base commune à l'ensemble des projets pour la rédaction de la politique de gestion des comptes et mots de passe d'une plateforme projet Amue.

06 MARS 2017

VERSIONS DU DOCUMENT

Version	Date	Émetteur	Statut/Suivi des modifications
1.00	06/03/2017	B. Chabal – C. Servaes	Initialisation du document
1.1	19/02/2024	DSSE – Pole technique	Revue et ajout d'annexes

DOCUMENTS ASSOCIES

Référence	Titre
ANSSI N°DAT-NT-001/ANSSI/SDE/NP	Recommandations de sécurité relatives aux mots de passe



TABLE DES MATIERES

1.	Introduction.....	3
2.	Nommage des comptes.....	4
2.1.	Les comptes techniques.....	4
2.2.	Les comptes nominatifs	4
2.3.	Les comptes applicatifs génériques	5
3.	Règles de création des mots de passe	5
3.1.	Création des mots de passe des comptes techniques	5
3.2.	Création des mots de passe des comptes nominatifs.....	5
3.3.	Création des mots de passe des comptes applicatifs génériques.....	5
3.4.	Création des mots de passe de chiffrement des échanges entre intervenants.....	5
4.	Règles et procédures de mises à jour des mots de passe.....	6
4.1.	Mises à jour des mots de passe des comptes techniques	6
4.2.	Mises à jour des mots de passe des comptes nominatifs.....	6
4.3.	Mises à jour du mot de passe des comptes applicatifs génériques	6
4.4.	Mises à jour des mots de passe de chiffrement des échanges entre intervenants	6
5.	Procédure de fourniture des comptes et des mots de passe aux utilisateurs ...	6
6.	Procédure de suppression des comptes utilisateurs	6
7.	Règles d'utilisation	6
A.	Annexes	7



1. Introduction

Ce document a pour objectif de décrire la base commune à l'ensemble des projets pour la rédaction de la politique de gestion des comptes et mots de passe d'une plateforme projet Amue.

Le périmètre de ce document est volontairement restreint aux environnements permettant de construire et maintenir une solution Amue, et ne couvre pas la solution elle-même.

Une telle politique a pour objectif de rassembler et de décrire l'ensemble des règles qui doivent s'appliquer en matière de gestion des comptes et des mots de passe sur une plateforme projet. Au moment d'instancier ce document de sécurité, le projet complètera les chapitres ci-dessous en fonction du contexte. Certaines mentions écrites en **vert** dans ce document ont été placées pour aider le projet dans la rédaction.

Une fois instancié, ce document confidentiel est à usage restreint et ne doit être diffusé qu'aux personnes ayant le besoin d'en connaître (personnels Amue et prestataires identifiés intervenant sur la plateforme projet).

Les différents sujets abordés ici sont :

- Le nommage des comptes
- Les règles de création des mots de passe
- Les règles de mises à jour des mots de passe
- La procédure de fourniture des comptes et des mots de passe aux utilisateurs
- La procédure de suppression des comptes utilisateurs
- Les règles d'utilisation de certains comptes

Pour faciliter la lecture du document, les règles sont référencées par les sigles : **Rx**



2. Nommage des comptes

Les identifiants utilisés sur une plateforme projet peuvent être classés dans différentes catégories. Ce chapitre a pour objectif de dresser une liste exhaustive des comptes utilisés et de préciser les règles qui doivent être respectées lors de la création de ces identifiants.

2.1. Les comptes techniques

Les comptes techniques sont de deux types, les comptes génériques créés au niveau des systèmes d'exploitation d'une part, et les comptes systèmes logiciels d'autre part.

Les comptes système d'exploitation sont les suivants :

- Le compte administrateur de chaque serveur Windows
- Le compte « root » de chaque serveur de type Unix
- ... A compléter (comptes pour l'installation du SGBD, Fusion Middleware, Tomcat, ...)

R1 <Première règle>.

R2 <Deuxième règle>.

Les comptes systèmes logiciels utilisés pour administrer les différentes briques logicielles nécessaires à la solution Amue sont :

- Ajouter ici la liste de tous les comptes systèmes logiciels permettant d'installer les briques logicielles de la solution Amue
- Exemple : les utilisateurs propriétaires des schémas applicatifs au sein des instances de base de données.
- Exemple : les comptes SYS, SYSTEM et autres pour chaque instance de base de données Oracle

S'il y a une règle de nommage permettant de définir des noms variables, il faut l'exposer ici.

2.2. Les comptes nominatifs

Ce chapitre a pour objectif d'expliquer les règles qui doivent être respectées lors de la création des comptes nominatifs des utilisateurs.

Les comptes nominatifs sont :

- Les comptes système d'exploitation pour les prestataires intervenant sur la plateforme projet,
- Les comptes applicatifs de la solution Amue pour chaque intervenant (technique, fonctionnel, personnel d'établissement, ...) sur la plateforme projet

R3 <Troisième règle>.

Rédiger ici les règles de construction des comptes applicatifs nominatifs.



2.3. Les comptes applicatifs génériques

Au sein de chaque applicatif permettant de construire les solutions Amue existent des comptes génériques ayant des profils d'habilitation différents.

La liste de ce type de comptes et des habilitations correspondantes est fixée par le projet et ne doivent pas être modifiées par le prestataire sans l'accord de l'Amue.

Ce chapitre a pour objectif de lister les comptes applicatifs génériques et de préciser les comptes ayant des droits étendus de type administration.

Dresser ici la liste des comptes.

3. Règles de création des mots de passe

3.1. Création des mots de passe des comptes techniques

Liste des exigences de complexité des mots de passe

Ces exigences de complexité sont appliquées lors du changement ou de la création de mots de passe. La complexité appliquée doit être en accord avec les contraintes définies par l'ANSSI.

3.2. Création des mots de passe des comptes nominatifs

Les utilisateurs d'un système d'information doivent être sensibilisés à l'utilisation de mots de passe forts afin de comprendre pourquoi le risque d'utiliser des mots de passe faibles peut entraîner une vulnérabilité sur le système d'information dans son ensemble et non pas sur leur poste uniquement.

Liste des exigences de complexité, d'expiration, de stockage des mots de passe.

3.3. Création des mots de passe des comptes applicatifs génériques

Si la solution le permet, les règles du chapitre précédent doivent être appliquées aux mots de passe des comptes applicatifs génériques.

Les mots de passe de ce type de comptes sont fixés par le projet et ne doivent pas être modifiés sans l'accord de l'Amue.

Liste des exigences de complexité, d'expiration, de stockage des mots de passe.

3.4. Création des mots de passe de chiffrement des échanges entre intervenants

Des mots de passe servant à chiffrer les échanges jugés sensibles entre les intervenants du projet doivent être convenus.

Ce type de mot de passe est strictement réservé aux seules personnes suivantes :

- < à compléter >



4. Règles et procédures de mises à jour des mots de passe

- 4.1. Mises à jour des mots de passe des comptes techniques
- 4.2. Mises à jour des mots de passe des comptes nominatifs
- 4.3. Mises à jour du mot de passe des comptes applicatifs génériques
- 4.4. Mises à jour des mots de passe de chiffrement des échanges entre intervenants

5. Procédure de fourniture des comptes et des mots de passe aux utilisateurs

Présentation des règles en matière de fourniture des comptes et des mots de passe.

6. Procédure de suppression des comptes utilisateurs

Le comité de suivi Amue-prestataire de chaque projet est informé de chaque modification de la liste des personnes autorisées à se connecter à la plateforme projet.

Lorsqu'un intervenant quitte le projet, les comptes nominatifs correspondants sont supprimés, et le projet procède éventuellement aux changements de certains mots de passe.

7. Règles d'utilisation

Présentation des règles d'utilisation de certains comptes.



A. Annexes

- Légifrance : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046432885>
- Références de l'ANSSI :
 - Guide d'hygiène informatique : https://cyber.gouv.fr/sites/default/files/2017/01/guide_hygiene_informatique_a_nssi.pdf
 - Bonnes pratiques : <https://cyber.gouv.fr/bonnes-pratiques-protégez-vous>
- Références CNIL :
 - Mots de passe : <https://www.cnil.fr/fr/mots-de-passe>
 - Mots de passe, nouvelle recommandation : <https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite>